Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0281-2005

for

JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0

from

Gemplus SA

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0281-2005

JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0

from

Gemplus SA

Common Criteria Arrangement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0005-2002** **Protection Profile BSI-PP-0006-2002**
Functionality:	**PP BSI-PP-0005-2002 and PP BSI-PP-0006-2002 conformant plus product specific extensions** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 augmented by** **ADV_IMP.2 (Implementation of the TSF)** **AVA_MSU.3 (Vulnerability assessment – Analysis and testing for insecure states)** **AVA_VLA.4 (Vulnerability assessment – Highly resistant)**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 22 December 2005

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 22 September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

This evaluation contains the components ADV_IMP.2 (Implementation of the TSF), AVA_MSU.3 (Vulnerability assessment – Analysis and testing for insecure states) and AVA_VLA.4 (Vulnerability assessment – Highly resistant) that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 has undergone the certification procedure at BSI.

The evaluation of the product JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 was conducted by the Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜVIT) which is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, and vendor and distributor is:

Gemplus SA
Avenue du Pic de Bertagne
Parc d'activités de Gémenos
13420 Gémenos
France

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 22 December 2005.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-34.

The product JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Gemplus SA
Avenue du Pic de Bertagne
Parc d'activités de Gémenos
13420 Gémenos
France

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The TOE is part of the product described below.

The product is an Open Platform Smart Card that provides Digital Signature creation services. As shown in Figure 1 (Figure 1 of [6]) the JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 is composed of:

- the Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30. The IC has been evaluated at EAL5+ level under the certification ID BSI-DSZ-CC-0315-2005. The TOE Security Target is build using the Security Functionality provided be the IC and the evaluation is build upon the results of the evaluation of the IC.
- specific IC Dedicated Software
- the Embedded Software of the GXP3 Platform
- ROMed application GemSAFE V2 digital signature application
- ROMed applications MPCOS[8] and GemSafe[9] (not part of the TOE)
- other ROMed applications (GemID[10], VSDC[11] and Dreifus[12]) which are deactivated during the Card Initialization phase and therefore cannot be personalized or used afterwards (not part of the TOE)

This certification does not include a confirmation according to the German Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations [30].

[8] MPCOS is a JavaCard Type application that provides Data Storage and e-purse services. MPCOS application relies on the GXP3 JavaCard platform and uses interoperable interfaces.

[9] GemSafe application is a JavaCard type application that provides also identity, digital signature and data storage services.

[10] GemID is a JavaCard type application that provides identification/authentication services.

[11] VSDC, VISA Smart Debit Credit application, is a JavaCard type application compliant with VISA specifications and provides EMV payment services.

[12] Dreifus application is a JavaCard type application that provides also Digital Signature services.

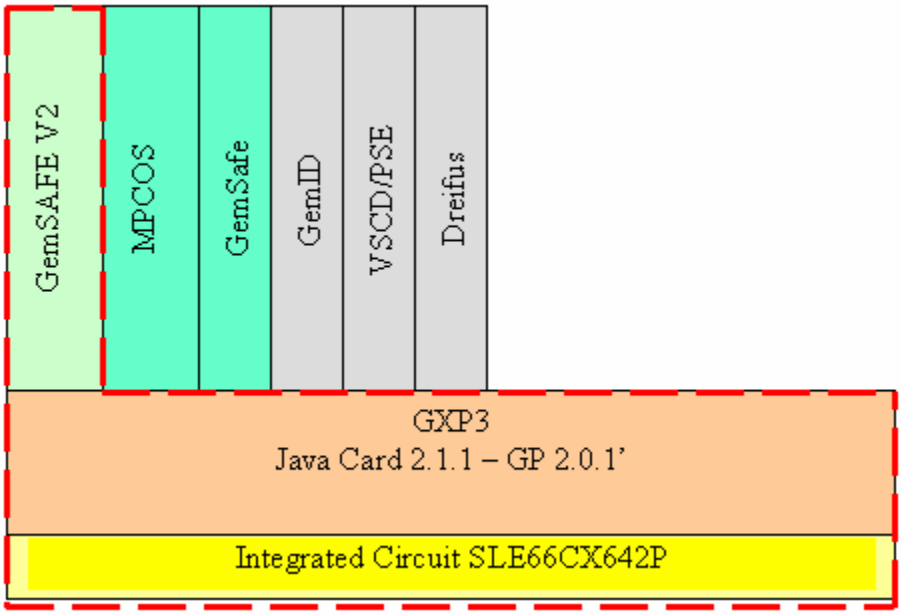

Figure 1: JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0

The TOE is limited to the Digital Signature provided by GemSAFE V2, the GXP3 services available to install and support GemSAFE V2, and the IC that supports the GXP3 platform. The scope of the TOE is marked by the red dashed line in Figure 1.

GemID, VSDC and Dreifus applications are locked during Card Initialization and cannot be installed or personalized. These applications are out of the scope of the TOE and the TOE environment.

The MPCOS and GemSafe applications are not part of the TOE either. These applications can be installed and personalized using GXP3 platform services. The platform ensures that these applications do not interfere with the GemSAFE V2 signature application.

GemSAFE V2 is a Java Card application that provides a Secure Signature Creation Device (SSCD). The GemSAFE V2 supports

- the generation of SCD/SVD pairs on-board (option b) [12] during the personalization process of the card, or
- the import of the SCD (option a) via a trusted channel [11]
- the generation of electronic signatures.

GemSAFE V2 features the following options:

- Generation of digital signature with PK or SK schemes
- Instantiation of Stand Alone applet

GemSAFE V2 is aimed to create legal valid signatures and therefore provides mechanisms to ensure the Secure Signature Creation as:

- authentication of the signatory
- authentication of the administrators
- integrity of access conditions to protected data

- integrity of the Data to be Signed
- external communication protection against disclosure and corruption (secure messaging)
- access control to commands and data by authorized users

The **GXP3** is a Java Open Platform that complies with

- Sun's Java Card 2.1.1, which consists of the Java Card 2.1.1 Virtual Machine, Java Card 2.1.1 Runtime Environment and the Java Card 2.1.1 Application Programming Interface
- the GlobalPlatform Card Specification Version 2.0.1 that defines the card management, enhanced by the additional security features described in the Open Platform 2.0.1 Visa Card Implementation Requirements Configuration 2 -compact with PK

The platform consists of the following components:

- the Operating System that provides the basic card functionalities, including DES and RSA algorithms, Hash algorithm, true random numbers and the cryptographic library
- the Java Card Runtime Environment, which provides a secure framework for the execution of Java Card programs and data access management (firewall)
- the Open Platform Card Manager, which provides card and application management functions and security control

The platform is built upon the SLE66CX642P/m1485b16 with RSA 2048 V1.30 IC (evaluated under the certification ID BSI-DSZ-CC-0315-2005) with a 64K EEPROM size. The EEPROM size can be limited to 36K by software configuration during personalization. The TOE has two configurations. One configuration with a 64K EEPROM and one configuration with 36K EEPROM.

The GXP3 platform will provide the following services:

- Initialization of the GP card Manager and management the GP Card Life Cycle
- Lock of the LOAD command to avoid loading of other applets in EEPROM in any life cycle state
- Secure installation of the application under Card Manager control
- Secure Messaging services during Applet personalization
- Extradition services to allow several Applet instances to share a dedicated Security Domain
- Deletion of application instances under Card manager control
- Secure operation of the Applet instances through Java Card/ API
- Card basic security services (as environmental operating conditions check through information provided by the IC, life cycle consistency check, integrity and confidentiality of keys in PIN stored for the applet, random number generation, secure data object handling and backup mechanisms, ROM and EEPROM integrity check, memory content management and mechanisms to prohibit other applets to interfere with GemSAFE V2 applet)

The IT product JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 was evaluated by the Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜVIT) which is an evaluation facility (ITSEF)[13] recognised by BSI.

The sponsor, and vendor and distributor is

Gemplus SA
Avenue du Pic de Bertagne
Parc d'activités de Gémenos
13420 Gémenos
France

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: ADV_IMP.2	Development – Implementation of the TSF
+: AVA_MSU.3	Vulnerability assessment – Analysis and testing for insecure states
+: AVA_VLA.4	Vulnerability assessment – Highly resistant

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The SFRs in the following 2 tables are taken from CC part 2. If an SFR is labeled with (option a) it means that it is taken from the SSCD Type 2 Protection Profile [11] and (option b) means it is taken from the SSCD Type 3 2 Protection Profile [12].

Security Functional Requirement	Addressed issue
FCS	**Cryptographic support**
FCS_CKM.1 (option b)	Cryptographic key generation
FCS_CKM.4 (option a)	Cryptographic key destruction

[13] Information Technology Security Evaluation Facility

Security Functional Requirement	Addressed issue
FCS_CKM.4 (option b)	Cryptographic key destruction
FCS_COP.1/CORRESP	Cryptographic operation/Correspondence verification
FCS_COP.1/SIGNING	Cryptographic operation /Digital signature verification
FCS_COP.1/DES	Cryptographic operation/DES
FDP	**User data protection**
FDP_ACC.1 (option a) SVD Transfer SFP	Subset access control /SVD Transfer SFP
FDP_ACC.1 (option b) SVD Transfer SFP	Subset access control/ SVD Transfer SFP
FDP_ACC.1 (option a) SCD Import SFP	Subset access control/ SCD Import SFP
FDP_ACC.1 (option b) Initialization SFP	Subset access control/ Initialization SFP
FDP_ACC.1 Personalization SFP	Subset access control/ Personalization SFP
FDP_ACC.1 Signature-creation SFP	Subset access control/ Signature-creation SFP
FDP_ACF.1 (option b) Initialization SFP	Security attribute based access control/ Initialization SFP
FDP_ACF.1 (option a, b) SVD Transfer SFP	Security attribute based access control/ SVD Transfer SFP
FDP_ACF.1 (option a) SCD Import SFP	Security attribute based access control/ SCD Import SFP
FDP_ACF.1 Personalization SFP	Security attribute based access control/ Personalization SFP
FDP_ACF.1 Signature-creation SFP	Security attribute based access control/ Signature-creation SFP
FDP_ETC.1/SVD Transfer	Export of user data without security attributes/SVD Transfer
FDP_ITC.1 /SCD (option a)	Import of user data without security attributes/SCD
FDP_ITC.1 /DTBS	Import of user data without security attributes/DTBS
FDP_RIP.1	Subset residual information protection
FDP_SDI.2/persistent	Stored data integrity monitoring and

Security Functional Requirement	Addressed issue
	action/persistent
FDP_SDI.2/DTBS	Stored data integrity monitoring and action/DTBS
FDP_UCT.1/Receiver (option a)	Basic data exchange confidentiality
FDP_UIT.1/SVD Transfer	Data exchange integrity/ SVD Transfer
FDP_UIT.1/TOE DTBS	Data exchange integrity/TOE DTBS
FIA	**Identification and authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1 (option a)	Timing of authentication
FIA_UAU.1 (option b)	Timing of authentication
FIA_UID.1 (option a)	Timing of identification
FIA_UID.1 (option b)	Timing of identification
FMT	**Security Management**
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1(option a) Administrator	Management of security attributes/ Administrator (option a)
FMT_MSA.1(option b) Administrator	Management of security attributes/ Administrator (option b)
FMT_MSA.1/Signatory	Management of security attributes/Signatory
FMT_MSA.2	Secure security attributes
FMT_MSA.3 (option a)	Static attribute initialization (option a)
FMT_MSA.3 (option b)	Static attribute initialization (option b)
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FPT	**Protection of the TOE Security Functions**
FPT_AMT.1	Abstract machine testing
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
FTP	**Trusted path/channels**
FTP_ITC.1(option a) SCD Import	Inter-TSF trusted channel / SCD Import (option a)
FTP_ITC.1(option a) SVD Transfer	Inter-TSF trusted channel /SVD Transfer (option a)

Security Functional Requirement	Addressed issue
FTP_ITC.1(option b) SVD Transfer	Inter-TSF trusted channel /SVD Transfer (option b)
FTP_ITC.1/DTBS Import	Inter-TSF trusted channel /DTBS Import
FTP_TRP.1/TOE	Trusted path

Table 2: Digital signature SFRs for the TOE taken from CC Part 2

Security Functional Requirement	Addressed issue
FAU	**Security audit**
FAU_ARP.1	Security alarms
FAU_SAA.1	Potential violation analysis
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation
FCS_CKM.3	Cryptographic key access
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operations
FDP	**User data protection**
FDP_ACC.1	Subset Access control
FDP_ACF.1	Security attributes based access control
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UCT.1	Basic data exchange confidentiality
FIA	**Identification and Authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT	**Security management**
FMT_MOF.1	Management of security function behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Function
FMT_SMR.1	Security roles

Security Functional Requirement	Addressed issue
FPT	**Protection of the TOE Security function**
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_RVM.1	Non bypassability of the TSP
FPT_SEP.1	TSF Domain separation
FPT_TDC.1	Inter TSF Basic TSF Data consistency
FPT_TST.1	TSF testing
FTP	**Trusted path/Channel**
FTP_TRP.1	Trusted Path

Table 3: Platform SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Addressed issue
FPT	**Protection of the TOE Security Functions**
FPT_EMSEC.1	TOE Emanation

Table 4: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.1 and 5.2.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.3	Cryptographic key access
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operations
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FTP	**Trusted path/Channel**
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

Table 5: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.4.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
Digital Signature TSF	
SF_SIG_AUTHENTICATION	Authentication management
SF_SIG_CRYPTO	Cryptography management
SF_SIG_INTEGRITY	Integrity
SF_SIG_MANAGEMENT	Management of operations & access control
SF_SIG_SECURE_MESSAGING	Secure messaging
Platform TSF	
SF_CARD_AUTHENTICATION	Card authentication
SF_CARD_CRYPTO	Card cryptographic algorithm & key management
SF_CARD_EMANATION	Emanation protection
SF_CARD_INTEGRITY	Card objects integrity
SF_CARD_MGR	Card Manager
SF_CARD_PROTECT	Card operation protection
SF_CARD_SECURE_MESSAGING	Card Secure Messaging

Table 6: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

There, the hardware TSF are also listed. It is stated that two of the hardware TSF, SEF2 (Phase management with test mode lock-out) and SEF8 (Memory Management Unit, MMU) are not used by the embedded software.

1.3 Strength of Function

The TOE's strength of functions is claimed high (SOF-high) for specific functions as indicated in the Security Target [6, chapter 6.1 and 8.3]. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The following assets and subjects were defined in the Security Target [6]:

Digital Signature assets	Addressed issue
D.SCD	SCD: private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).
D.SVD	SVD: public key linked to the SCD and used to perform an electronic signature verification (integrity of the SVD when it is exported must be maintained).
D.DTBS	DTBS and DTBS-representation: set of data or its representation which is intended to be signed (their integrity must be maintained).
D.VAD	VAD: PIN code data entered by the end user to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed).
D.RAD	RAD: Reference PIN code authentication reference used to identify and authenticate the End User (Integrity and confidentiality of RAD must be maintained).
D.SIGN_APPLI	Signature-creation function of the SSCD using the SCD: (The quality of the function must be maintained so that it can participate to the legal validity of electronic signatures).
D.SIGNATURE	Electronic signature: (unforgeability of electronic signatures must be assured).

Table 7: Digital Signature assets

Platform assets	Addressed issue
D. CODE	Executable code ROMed on the platform or patch loaded in EEPROM, including ROMed applet code.
D.GP_KEYS	FAB_KEY loaded by the IC manufacturer to authenticate the Card Manufacturer during phase 4 and 5 b.
D.GP_ REGISTRY	GP registry that contains Card Manager data for Card management operations.
D.ISD_DATA	Issuer Security Domain Data.
D.ISD_KEYS	Issuer Security Domain Keys: Card Manager keys used during Applet initialization and card personalization. Includes keys for Authentication, Encryption and Integrity (MAC).
D.SD_DATA	Application Security Domain Data.
D.SD_KEYS	Application Security domain keys, includes Static Keys for secure channel operation (authentication) and keys for cryptographic operations (cipher, MAC) during a session.
D.USER_PIN	Application User Pin. For the application GemSAFE V2 this data is the D.VAD.
D.JAVA_OBJECT	Data Object belonging to an application identified with its SD.

Table 8: Platform assets

Digital signature subjects	Addressed issue
S.User	End user of the TOE which can be identified as S.Admin or S.Signatory.
S.Admin	User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions.
S.Signatory	User who holds the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents.
S.OFFCARD	Attacker. A human or process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a high level potential attack and knows no secret.

Table 9: Digital signature subjects

Platform subjects	Addressed issue
S.Card_Manufacturer	Administrator of the TOE, which can be identified as the Card Manufacturer. This entity is in charge of Platform initialization, installation of the Issuer Security Domain (ISD) and set the platform to OP_READY state.
S.Card_Manager	This entity represent the Open Platform Card Issuer, manages the card content and controls application privileges. This entity will install/delete application instances and manage the card life-cycle.
S. Applet	Any application ROMed on the platform and using platform services.
S.OFFCARD	Attacker. A human or process acting on his behalf being located outside the TOE. The main goal of the S.OFFCARD attacker is to access Application sensitive information. The attacker has a high level potential attack and knows no secret.

Table 10: Platform subjects

Threats and Organisational Security Policies (OSPs) which were assumed for the evaluation and averted by the TOE are specified in the Security Target [6]:

Digital Signature threats	Addressed issue
T.Hack_Phys	Physical attacks through the TOE interfaces. An attacker S.OFFCARD interacts with the TOE interfaces to exploit vulnerabilities to gain fraudulent access to the assets.
T.SCD_Divulg	Storing, copying, and releasing of signature-creation D.SCD. An attacker S.OFFCARD can store, copy the SCD D.SCD outside the TOE. An attacker S.OFFCARD can release the SCD D.SCD during generation, storage and use for signature-creation in the TOE.
T.SCD_Derive	Derive the signature-creation data D.SCD.

Digital Signature threats	Addressed issue
	An attacker S.OFFCARD derives the SCD D.SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.
T.Sig_Forgery	Forgery of electronic signature D.SIGNATURE. An attacker S.OFFCARD forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.
T.Sig_Repud	Repudiation of signatures D.SIGNATURE. If an attacker S.OFFCARD can successfully threaten any of the assets, then the non repudiation of the electronic signature is compromised. The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.
T.SVD_Forgery	Forgery of the signature- verification data D.SVD. An attacker S.OFFCARD forges the SVD D.SVD presented by the TOE. This result in loss of SVD integrity in the certificate of the signatory.
T.DTBS_Forgery	Forgery of the DTBS-representation D.DTBS. An attacker S.OFFCARD modifies the DTBS-representation D.DTBS. sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intends to sign.
T.SigF_Misuse	Misuse of the Signature-Creation function of the TOE D.SIGN_APPLI . An attacker S.OFFCARD misuses the signature-creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

Table 11: Digital Signature threats

Platform threats	Addressed issue
T.Plt_Integrity	Integrity of Platform Data and code S.OFFCARD tries to alter Platform stored sensitive data (assets) or code to gain access to unauthorized data or operations. This threat concerns D.GP_KEYS, D.ISD_KEYS, D.SD_KEYS and D.CODE.

Platform threats	Addressed issue
T.Plt_Confidentiality	Confidentiality of Platform Data S.OFFCARD tries to disclose Platform stored Data to gain access to unauthorized operations. This threat concerns D.GP_KEYS, D.ISD_KEYS, D.SD_KEYS.
T.Plt_Install	S.OFFCARD fraudulently install an applet on the card. This concerns either the installation of an unauthorized applet or an attempt to induce a malfunction in the TOE through the installation process. This threat concerns applets installation and mainly D.GP_REGISTRY, D.SD_DATA and D.SD_KEYS.
T.Plt_Execution	S.OFFCARD or S.APPLET executes code in order to gain illegal access to platform or applet resources. This threat deals with D.CODE access.
T.Plt_Operate	S.OFFCARD or S.APPLET tries to modify Platform behavior by unauthorized or incorrect use of commands, or by producing malfunction conditions. This includes bad command, authentication bypass, insecure state by insertion or interruption of session. This threat concerns all platform assets.

Table 12: Platform threats

Digital Signature OSPs	Addressed issue
P.CSP_Qcert	Qualified certificate. The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.
P.Qsign	Qualified electronic signatures. The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is created by a SSCD.
P.Sigy_SSCD	TOE as secure signature-creation device. The TOE stores the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

Table 13: Digital Signature OSPs

Platform OSPs	Addressed issue
P.Plt_Support	The platform allows the Digital Signature application to operate in a secure environment. The platform will support: - Secure Digital Signature application installation and extradition, - Secure deletion of Digital Signature instantiation, - Secure operating environment with detection of environmental trouble shooting, - Secure execution environment and data sharing. The Platform shall provide cryptographic services for the applet as RSA and DES.
P.IC_Support	This IC is the Infineon SLE66CX642P, used by the platform shall be CC certified at a level comparable to the level of the current TOE evaluation: EAL4+. The IC shall support the security of the TOE operating environment and provide protection against - Physical manipulation of the IC, - Physical Probing of the IC, - Malfunction due to environment stress, - Inherent or forced information leakage, - Deficiency of Random Numbers.
P.Applet_conformity	Other instanciable Applets, ROMed on the Platform but not part of the TOE shall comply with Java Card 2.1.1 and GP 2.0.1. Appropriate instruction on the install of these applications shall be supplied with the TOE.

Table 14: Platform OSPs

1.5 Special configuration requirements

The TOE is a Secure Signature Creation Device. It is defined uniquely by the name and version number product JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0. Its implementation representation and its configuration are specified by the Configuration List (Data List [27], Card Software Configuration Check [28] and Configuration Items History G148 [29]).

The TOE as a Secure Signature Creation Device for key generation and signature creation is built upon the SLE66CX642P/m1485b16 with RSA 2048 V1.30 IC with a 64K EEPROM size. The EEPROM size can be limited to 36K by software configuration during Card Initialization flow, which is part of the installation process. Therefore, the TOE has two platform configurations defined in [6, chapter 2.2.1] and was tested in both configurations:

- GXP3.2-E64PK-CC with 64K EEPROM

- GXP3.2-E64PK-CC with 36K EEPROM

The evaluation and subsequent certification are therefore only valid for these configurations of the TOE JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0.

As outlined in chapter 1 of this report and listed in line 2, table 15 in chapter 2 of this report, there are other applications on the product: MPCOS, GemSafe, GemID, VSDC and Dreifus. The TOE was tested together with these applications and the evaluation results are restricted to chip cards containing the TOE with those applications.

The TOE supports both the import of the SCD via a trusted channel (SSCD type 2, [11]) and the generation of SCD/SVD pairs on-board (SSCD type 3, [12]).

The TOE is delivered after IC initialisation, at the end of phase 3 of the open platform life cycle, see [6, chapter 2.3]. Phases 4 to 7 are covered by guidance for installation and start-up:

- Phase 4 – IC Packaging
  IC Packaging guidance (phase 4) [13, chapter 3.4] including ATR
- Phase 5a – Card initialization
  Card manufacturer's guidance (phase 5) [13, chapter 3.5]
  Card Initialization specification [13, chapter 3.5.1]
  Card Initialization Specification [17] and Flow Description [17, chapter 4]
  Initialization flow description [18, chapter 3]
- Phase 5b – Applet Install
  GemSafe V2 installation guidance (phase 5b) [14, chapter 3.3.1]
  Installing the GemSafe V2 Applet [15, chapter 4]
- Phase 6 – Applet personalization
  GemSafe V2 personalization guidance (phase 6) [14, chapter 3.3.2]
  Personalizer guidance (phase 6) [13, chapter 3.6]
  Personalizing the GemSafe V2 Applet [15, chapter 5]
  Personalization Phase Commands [15, chapter 10]
  Personalization Constraints [19]
- Phase 7 – Product end-usage
  GemSafe V2 Post-issuance Guidance (phase7) [14, chapter 3.3.3]
  Card Issuer and Post-Issuance Guidance (phase 7) [13, chapter 3.7]
  Application Phase Commands [15, chapter 11]
  Recommendation to end user (phase 7) [13, chapter 4.3] for PIN usage and Smart Card

The end user receives the TOE in an operational state where installation and generation procedures cannot be reapplied and the only start-up procedures applied by the end user is a change of the signatory PIN before the end user

can first use the TOE to create signatures [15, chapter 11, PSO-Compute Digital Signature].

Recommendations and hints for the user are provided in the user guidance [14, chapter 4.3]:

The end user is the card holder to which the card is issued for signature application. The card is issued to the card holder by the Card Issuer during phase 7. From that moment the Smart card is in card holder's care until the card is permanently disabled or destroyed.

End user Guidance recommendation to the Card Issuer:

- The Card Issuer should provide a user guidance to the card holder. This guidance should contain all appropriate recommendations to the card holder to use and keep his card in a secure way and especially the following information. The card issuer should also require the Signatory to follow the provided guidance.

PIN recommendations to End user (phase7)

- The Personal Identification Number (PIN) is required to identify the user's identity and to protect the fraudulent usage of a card that would be lost and/or stolen,
- The card holder is the only person to know the PIN value,
- The card holder must keep the PIN value strictly confidential and is responsible for it.
- The PIN value should be is at least 6 digits long. When the signatory changes the PIN, the value should be sufficiently diversified.

Card recommendation to end user (phase 7)

- The card may become out of service for reasons like: Card expired, PIN wrong, presentation surpassed the authorized ratification counter value (3 times), Card is blocked, Card is broken and cannot be read any longer, Card is in Terminated stage after severe security fault detection.
- In such cases, the card should be brought to the Issuer or Issuer representative for a safe recovery or destruction process.
- If the card is stolen or lost, the card holder should declare as soon as possible to the issuer.

Signature usage recommendation to end user (phase 7)

- For a high-security certified signature application (Common Criteria certification) the "Change PIN before first use" option, is mandatory.
- For such a high-security product, the end user must verify that the card received from the card issuer has never been used to generate a signature before.

- In order to proceed to this verification, the end user should perform the following steps:

  1. Perform a PIN verification using the PIN received by mail from the card issuer.
  2. Sign a message. The signing operation fails.
  3. Change the PIN as required.
  4. Verify the new PIN.
  5. Sign a message. The signing operation is successful.

  This check if the TOE has not been previously used for signing to be performed by the user is also addressed in the delivery to the TOE final user, the signatory, described in [20, chapter 3.2.5]:
  The card issuer delivers the card to the final user protected by an initial PIN. After receiving the card and the PIN, the user verifies that the card has not been previously used for signing and changes the PIN by applying the procedure suggested in [14, chapter 4.3.3] and [15, chapter 4] following table 18. The usage of the signature application by the signatory is protected by the signatory PIN and the signatory has to keep his PIN value secret as required by end user recommendations concerning the PIN usage in [14, chapter 4.3.1].

Detailed information about specific security characteristics of key, PIN and hash values that are under the control of TSF is provided in the Personalization Constraints [19].

1.6 Assumptions about the operating environment

The following constraints concerning the operating environment are made in the Security Target, please refer to the Security Target [6], chapter 3.4:

Digital Signature assumptions

- A.CGA: Trustworthy certification-generation application
  The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.
- A.SCA: Trustworthy signature-creation application
  The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.
- A.SCD_Generate (option a): Trustworthy SCD/SVD generation
  If a party other than the signatory generates the SCD/SVD-pair of a signatory, then
  (a) this party will use a SSCD for SCD/SVD-generation,
  (b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and
  (c) the SCD will not be used for signature-creation until the SCD is under the

sole control of the signatory.
(d) The generation of the SCD/SVD is invoked by authorized users only.
(e) The SSCD Type 1 ensures the authenticity of the SVD it has created and exported.

Platform assumptions

- A.No_Loading
  It is assumed that there is no loading of applets after the TOE delivery at the end of phase 3.

- A.Plt_Process
  It is assumed that, after TOE delivery, Security Procedures are used by Card Manufacturer and Card Issuer (phase 4 to 6) during delivery and storage for protection of the TOE material/information.
  It is assumed that security procedures are used during all manufacturing and test operations through phase 4 to 6, to maintain confidentiality and integrity of the TOE and of its manufacturing and test data, to prevent any possible copy, modification, retention, theft or unauthorized used.
  It is assumed that appropriate functionality testing of the TOE is used in phases 4, 5 and 6.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	JavaCard Platform consisting of - Micro Controller SLE66CX642P/m1485b16 with RSA 2048 V1.30		Modules
	SW	- Embedded Software GXP3.2-E64PK-CC	3.2	Software in ROM and EEPROM

No	Type	Identifier	Release	Form of Delivery
2	SW	- MPCOS version 3.01 - GemSafe version 1.11 - GemID version 1.02 - VSDC /PSE version 2.5 - GS-CIS Dreifus C3 Applet Version 1.0.0.0		Software in ROM and EEPROM
3	SW	Digital Signature application GemSAFE V2	V2	Software in ROM and EEPROM
4	DOC	Card Initialization Specification For GemXpresso Pro R3.2 E64 PK CC	A13	Document in paper / electronic form [17]
5	DOC	Functional Requirements Specification Initialization flow description for GXP3.2 E64PK CC and PPP 36K	A24	Document in paper / electronic form [18]
6	DOC	Personalization Constraints For GXP3-CC -GemSafe V2	A03	Document in paper / electronic form [19]
7	DOC	Administrator & User Guidance GXP3-CC, TOE - GXP3.2- E64PK-CC GemSAFE V2, Product - GXP3.2-E64PK-CC	0.3	Document in paper / electronic form [13]
8	DOC	Administrator & User Guidance GemSafe V2, TOE - GXP3.2- E64PK-CC GemSAFE V2, Product - GXP3.2-E64PK-CC	0.3	Document in paper / electronic form [14]
9	DOC	GemSafe V2 Applet Reference Manual	5	Document in paper / electronic form [15]
10	DOC	GemXpresso Pro R3.x Reference Manual	3	Document in paper / electronic form [16]
11	DOC	MPCOS Applet 2.0 Reference Manual	1.0	Document in paper / electronic form [21]
12	DOC	GemID Reference Manual	1.0	Document in paper / electronic form [22]
13	DOC	GEMSAFE Applet Reference Manual	3	Document in paper / electronic form [23]
14	DOC	TDS_TG Technical Design Specification For T=G protocol	A00	Document in paper / electronic form [24]

Table 15: Deliverables of the TOE

The delivery process after phase 4 uses the following mechanisms and procedures to allow detection of masquerading between administrators and the TOE user:

- Defined delivery flow and Card Initialization process and personalization processes
- Protection of the smart card by card manager keys
- Protection of the smart card's signature application by a PIN

3 Security Policy

The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software and will intended to be used as a Secure Signature Creation Device (SSCD) for the generation of signature creation data (SCD) and the creation of qualified electronic signatures.

This certification does not include a confirmation according to the German Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations [30].

The security policy of the platform is to provide

- authentication management for the administrator and administration of the card during its life-cycle
- card cryptographic algorithms and keys management
- protection of the digital signature application data against snooping
- checks of the integrity of the cryptographic keys, digital signature persistently stored data and the card life cycle state
- protection of the TSF
- the integrity and the confidentiality of command messages transmission in a secure channel

The security policy of the digital signature application GemSAFE V2 is to provide

- authentication management including authentication operations for secure channel management
- cryptographic operations of the digital signature application, including destruction of previous cryptographic keys
- monitoring of the integrity of user data and integrity of the DTBS, prohibition of the use of altered data and informing S.Signatory about integrity errors
- management of operations and access
- the integrity and confidentiality of user data exchanged

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Specific usage assumptions were not addressed by this product evaluation.

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [6, chapter 3.4]):

- The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP (A.CGA).
- The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE (A.SCA).
- If a party other than the signatory generates the SCD/SVD-pair of a signatory, then
  (a) this party will use a SSCD for SCD/SVD-generation,
  (b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and
  (c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.
  (d) The generation of the SCD/SVD is invoked by authorized users only
  (e) The SSCD Type 1 ensures the authenticity of the SVD it has created and exported (A.SCD_Generate).
- It is assumed that there is no loading of applets after the TOE delivery at the end of phase 3 (A.No_Loading).
- It is assumed that, after TOE delivery, Security Procedures are used by Card Manufacturer and Card Issuer (phase 4 to 6) during delivery and storage for protection of the TOE material/information.
  It is assumed that security procedures are used during all manufacturing and test operations through phase 4 to 6, to maintain confidentiality and integrity of the TOE and of its manufacturing and test data, to prevent any possible copy, modification, retention, theft or unauthorized used.
  It is assumed that appropriate functionality testing of the TOE is used in phases 4, 5 and 6. (A.Plt_Process).

Furthermore, the Security Target [6, chapter 3.5.1] defines three Organisational Security Policies for the Digital Signature Application that state that the CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD (P.CSP_Qcert), that the signatory uses a signature creation system to sign data with a qualified electronic signature that is based on a qualified certificate and that is created by an SSCD (P.Qsign), and that the TOE implements the SCD used for signature creation under sole control of the signatory (P.Sigy_SSCD).

There are also three Organisational Security Policies for the Smart Card Platform [6, chapter 3.5.2]. They state that the platform allows the Digital Signature application to operate in a secure environment (P.Plt_Support), that the Smart Card IC used by the platform shall be CC certified at a level comparable to the level of the TOE evaluation (P.IC_Support) and other instanciable Applets, ROMed on the Platform but not part of the TOE shall comply with the used standards and appropriate instruction on the install of these applications shall be supplied with the TOE (P.Applet_conformity).

Please refer to the Security Target [6, chapter 3.5] for more detail.

4.3 Clarification of scope

Additional threats that are not countered by the TOE and its evaluated security functions were not addressed by this product evaluation.

5 Architectural Information

The TOE (JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0) is a secure signature creation device comprising an integrated circuit (IC) with an operating system (OS) and a signature application. An overview of the architecture is given in chapter 1 of this report (including Figure 1, a top level block diagram of the JavaCard Platform GXP3.2-E64PK-CC) and chapter 2 of the Security Target [6], where also a top level block diagram of the GXP3 platform architecture can be found. A top level block diagram of the hardware IC including an overview of subsystems can be found within the TOE description of the Security Target of the chip [9].

6 Documentation

The documentation which is provided by the developer is listed in table 15 of this report and discussed in more detail in chapter 1.5 of this report.

7 IT Product Testing

Tests of the TOE were done (i) with real cards using a card reader and a PC, (ii) on a ROM monitor for destructive test of the TOE leading to a life cycle state TERMINATED and (iii) on an emulator where tests required break points and monitoring of memory cells during operation in an emulator test environment.

Developer’s Tests:

For developer tests, the test cases were mapped to Security Functions. All Security Functions with their security properties and their interfaces were covered. In addition, the test cases were mapped to subsystems of the High-Level Design and to modules of the Low-Level Design. All subsystems and modules with their security properties and their interfaces were covered. The developer tested each property of the design specification. All command APDU

with valid and invalid inputs are tested and all functions are tested with valid and invalid inputs. All test results were documented in log-files. All security functions were tested with overall positive results.

Independent evaluator tests:

The tests of the evaluator were performed by ISO-7816 APDU command sequences using a real card as well as tests on a ROM monitor and with emulators. For sample testing the evaluator has decided to perform as many tests as possible or nearly all of the developer's functional testing performed. The evaluator conducted penetration testing on identified potential vulnerabilities. The TOE proved to be resistant against high attack potential.

Side channel attacks on DES and RSA were tested and analysed during the evaluation of the IC SLE66CX642P/m1485b16 with RSA 2048 V1.30 (BSI-DSZ-CC-0315-2005). The result of these analysis is still valid.

8 Evaluated Configuration

The TOE is delivered after phase 3, i.e. after IC initialisation at the hardware manufacturer. It is defined uniquely by the name and version number JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0.

The TOE has two configurations of the platform specified in the ST [6, chapter 2.2.1]:

- TOE configuration GXP3.2-E64PK-CC with 64K EEPROM (ATR historical byte T8 = 04 in [17, chapter 2], [18, chapter 3.5.1]),
- TOE configuration GXP3.2-E64PK-CC (PPP36K) with 36K EEPROM (limited to 36K by software configuration during personalization by ATR historical byte T8 = 03 in [17, chapter 2], [18, chapter 3.5.1]).

The evaluation results are restricted to chip cards containing the TOE with applications that have been inspected during the evaluation process and that are listed in chapter 1 of this report and in line 2, table 15 in chapter 2 of this report.

The TOE supports both the import of the SCD via a trusted channel (SSCD type 2, [11]) and the generation of SCD/SVD pairs on-board (SSCD type 3, [12]).

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34]).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 (see [4]) were used. For specific methodology on random number generator evaluation the scheme interpretations AIS 20 and AIS 31 (see [4]) were used.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Development tools CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Semiformal functional specification	ADV_FSP.2	PASS
Semiformal high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Semiformal correspondence demonstration	ADV_RCR.1	PASS
Formal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS

Assurance classes and components		**Verdict**
Sufficiency of security measures	ALC_DVS.1	PASS
Standardised life-cycle model	ALC_LCD.1	PASS
Compliance with implementation standards	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: low-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Analysis and testing for insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 16: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conform to the PPs BSI-PP-0005-2002T [11] and BSI-PP-0006-2002T [12],
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended,
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by
  ADV_IMP.2 (Implementation of the TSF),
  AVA_MSU.3 (Vulnerability assessment – Analysis and testing for insecure states) and
  AVA_VLA.4 (Vulnerability assessment – Highly resistant).
- the following TOE Security Functions fulfil the claimed Strength of Function: SF_SIG_AUTHENTICATION and SF_CARD_AUTHENTICATION were evaluated to fulfil the minimum strength level SOF-high defined in [6].
  The random number generator part of SF_CARD_CRYPTO was evaluated to fulfil [4, AIS 20] class K3 requirements with strength HIGH.
  Therefore the scheme interpretations AIS 20, AIS 26 and AIS 31 (see [4]) were used. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

The underlying hardware had been successfully assessed by the Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (TÜViT).

The results of the evaluation are only applicable to the JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 as outlined in chapter 2 and chapter 8 of this report and is produced and initialised in an environment that

was subject to an audit in the cause of the evaluation. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documentation (refer to chapter 6 of this report) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [6] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the Security Target [7] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete security target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

AIS Application Notes and Interpretation of the Scheme

APDU Application Protocol Data Unit, interface standard for smart cards, see ISO/IEC 7816 part 3

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

CA Certification Authority (part of a CSP)

CEM Common Methodology for IT Security Evaluation

CGA Certification Generation Application

CC Common Criteria for IT Security Evaluation

CSP Certification Service Provider

DPA Differential Power Analysis, an attack, which may compromise cryptographic keys by analysing the power consumption of the smart card chip

DF	Dedicated File, directory on a smart card file system according to ISO/IEC 7816
DRNG	Deterministic Random Number Generator (a term used and introduced in AIS 20)
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory; EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge
ETR	Evaluation Technical Report
FSP	Functional Specification
HLD	High-Level Design
IC	Integrated Circuit
IT	Information Technology
MF	Master File, top level directory (root) on a smart card file system according to ISO/IEC 7816
MMU	Memory Management Unit
OS	Operating System
OSP	Organisational Security Policy
PC	Personal Computer
PIN	Personal Identification Number
PP	Protection Profile
PROM	Programmable Read-Only Memory, a memory chip on which data can be written only once
PUK	Personal Unblock Key
RA	Registration Authority (part of a CSP)
RAD	Reference Authentication Data
RNG	Random Number Generator
RSA	Asymmetric crypto algorithm by R. L. Rivest, A. Shamir, L. Adleman
SCA	Signature Creation Application
SCD	Signature Creation Data
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement

SOF	Strength of Function
SSCD	Secure Signature Creation Device
ST	Security Target
SVAD	Signatory's Verification Authentication Data
SVD	Signature Verification Data
SW	Software
TOE	Target of Evaluation
TRNG	True Random Number Generator (a term used and introduced in AIS31)
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
VAD	Verification Authentication Data

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Dreifus - is a JavaCard type application on the JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 that provides Digital Signature services.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

GemID - a JavaCard type application on the JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 that provides identification/authentication services.

GemSafe - is a JavaCard type application on the JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 that provides identity, digital signature and data storage services.

Informal - Expressed in natural language.

MPCOS - JavaCard Type application on the JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 that provides Data Storage and e-purse services. MPCOS application relies on the GXP3 JavaCard platform and uses interoperable interfaces.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

VSDC (VISA Smart Debit Credit application) - a JavaCard type application on the JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 compliant with VISA specifications and provides EMV payment services.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS), e.g.

AIS 20: Functionality classes and evaluation methodology for deterministic random number generators AIS 20, Version 1, 2 December 1999

AIS 25 for: CC-Supporting Document: The application of CC to Integrated Circuits, Version 2, July 2002

AIS 26 for: CC-Supporting Document: Application of Attack Potential to Smartcards, Version 2, August 2002

AIS 31: Functionality classes and evaluation methodology of physical random number generators, Version 1, 25 September 2001

AIS 32: Use of the international approved CC Final Interpretations into the German Certification Scheme, Version 1, 2 July 2001

AIS 34: Evaluation Methodology for CC Assurance Classes for EAL5+, Version 1.00, 1 June 2004

AIS 35 for: CC-Supporting Document: ST-lite, Version 1.1, July 2002

AIS 36 for: CC-Supporting Documents: ETR-lite for Composition, Version 1.1, July 2002

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-CC-0281, Version 0.93, 03.11.2005, ASE - Security Target, TOE - GXP3.2-E64PK-CC GemSafe V2, Product - GXP3.2-E64PK-CC, SSCD Type 2 (option a) and SSCD Type 3 (option b), Gemplus (confidential document)

[7] Security Target BSI-DSZ-CC-0281, Version 1.0, 14.11.2005, ASE - Security Target, TOE - GXP3.2-E64PK-CC GemSafe V2, Product - GXP3.2-E64PK-CC, SSCD Type 2 (option a) and SSCD Type 3 (option b), Gemplus (sanitized public document)

[8] Evaluation Technical Report, Version 2, Document ID: 20642118_TÜViT_24.2, 10.11.2005, Evaluation Technical Report (ETR) (confidential document)

[9] Security Target BSI-DSZ-CC-0315, Version 1.2, 20.04.2004, Security Target for SLE66CX642P/m1485b16 (Drs) with RSA2048 V1.30, Infineon Technologies AG,

[10] Certificate for the Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software from Infineon Technologies AG; Deutsches IT-Sicherheitszertifikat, BSI-DSZ-CC-0315-2005, Bundesamt für Sicherheit in der Informationstechnik, 12.08.2005

[11] Protection Profile - Secure Signature-Creation Device (SSCD-PP) Type 2, Version 1.04, EAL 4+, BSI-PP-0005-2002T, 03.04.2002

[12] Protection Profile - Secure Signature Creation Device (SSCD-PP) Type 3, Version 1.05, EAL 4+, BSI-PP-0006-2002T, 03.04.2002

[13] Administrator & User Guidance GXP3-CC, TOE - GXP3.2-E64PK-CC GemSAFE V2, Product - GXP3.2-E64PK-CC, Version 0.3, 09.08.2005, Gemplus (confidential document)

[14] Administrator & User Guidance GemSafe V2, TOE - GXP3.2-E64PK-CC GemSAFE V2, Product - GXP3.2-E64PK-CC, Version 0.3, 06.09.2005 Gemplus (confidential document)

[15] GemSafe V2 Applet Reference Manual, Version 5, 30.09.2005, Gemplus

[16] GemXpresso Pro R3.x Reference Manual, Version 3, 08.07.2005, Gemplus

[17] Card Initialization Specification For GemXpresso Pro R3.2 E64 PK CC, Version A13, 20.09.2005, Gemplus (confidential document)

[18] Functional Requirements Specification Initialization flow description for GXP3.2-E64PK-CC and PPP 36K, Version A24, 15.09.2004, Gemplus (confidential document)

[19] Personalization Constraints For GXP3-CC GemSafe V2, Version A03, 20.09.2005, Gemplus (confidential document)

[20] Delivery & Operation, TOE - GXP3.2- E64PK-CC GemSAFE V2, Product - GXP3.2-E64PK-CC, Version 0.5, 20.09.2005, Gemplus (confidential document)

[21] MPCOS Applet 2.0 Reference Manual, Version 1.0, 11.10.2002, Gemplus

[22] GemID Reference Manual, Version 1.0, 11.10.2002, Gemplus

[23] GEMSAFE Applet Reference Manual, Version 3, 22.06.2004, Gemplus

[24] Technical Design Specification For T=G protocol, Version A00, 30.08.2005, Gemplus (confidential document)

[25] Configuration Management, TOE - GXP3.2-E64PK-CC GemSAFE V2, Product - GXP3.2-E64PK-CC, Version 0.3, 27.09.2005, Gemplus (confidential document)

[26] Master CMP For GemXpresso Pro R3 CC, Version A08, 25.01.2005, Gemplus (confidential document

[27] Data List (DAL01A10190G), Version A02, 30.09.2004, Gemplus (confidential document)

[28] Card Software Configuration Check for GXP3-CC, Version A07, 2.05.05, Gemplus (confidential document)

[29] Configuration Items History G148 (CI_History_G148_G146_for_TUVIT.xls), 02.08.2005, Gemplus (confidential document)

[30] German Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations: Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG), 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 1 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04. Januar 2005 (BGBl. I S. 2))

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Assurance categorisation (chapter 2.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 2.1."

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 17: Assurance family breakdown and map

Evaluation assurance levels (chapter 6)

"The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 18: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

"Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

"Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.“

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

"Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

"Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

"Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

"Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

"Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

"Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.“

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.“

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.“

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“